DOI: 10.3745/KIPSTC.2009.16C.6.669

해쉬된 태그ID와 대칭키 기반의 RFID 인증프로토콜

박 용 수[†] · 신 주 석[††] · 최 명 실[†††] · 정 경 호[††††] · 안 광 선[†††††]

요 약

무선으로 대상물의 고유정보를 인식함으로 대상물을 관리할 수 있게 하는 RFID(Radio Frequency Identification)기술은 유비쿼터스 시대의 핵심기술이다. RFID에서 정보는 공간상에서 쉽게 노출될 수 있음으로 보안 및 프라이버시 문제가 항시 존재한다. 본 논문에서는 저가형 태그의 구현에 적합한 대칭키 기반의 상호인증 프로토콜을 제안한다. 제안한 프로토콜은 대칭키를 사용하여 하드웨어 자원을 최소화할 수 있으며, 해쉬 함수로 암호화한 태그 ID를 사용하고 PUF(Physically Unclonable Function)의 Challenge-Response값을 공유 대칭키로 활용하기 때문에 키 노출 위험이 없는 안전한 프로토콜이다.

키워드 : RFID, 대칭키, 해쉬 함수, 인증 프로토콜, PUF

An RFID Authentication Protocol based Symmetric Key using Hashed Tag ID

Yong Soo Park[†] · Ju Seok Shin[††] · Myung Sil Choi[†††] · Kyung Ho Chung[††††] · Kwang Seon Ahn[†††††]

ABSTRACT

By identifying the unique information of the objects using the RF, the RFID technique which will be able to manage the object is spot-lighted as the main technology in Ubiquitous era. On RFID systems, since the information of RFID may easily be unveiled in air, the secure and privacy problems always exist. In this paper, we propose mutual authentication protocol based on symmetric key. Proposed protocol has been able to minimize the tag's H/W resource by using symmetric key. And we use tag ID which is encrypted with hash function and a shared symmetric key by Challenge-Response pair of PUF(Physically Unclonable Function), thus there is no key disclosure problem in our protocol.

Keywords : RFID, Symmetric Key, Hash Function, Authentication protocol, PUF

1. 서 론

무선을 이용하여 대상물의 고유정보를 인식함으로, 대상물을 관리할 수 있게 하는 RFID(Radio Frequency Identification)기술은 유비쿼터스 시대의 핵심기술로써 각광을 받고 있다. 이 기술은 공간을 통하여 임의의 반경 내의 사물에 동시에 접근할 수 있는 전자파의 특성을 이용하기 때문에 대상물의 정렬 불필요, 빠른 재고 조사, 아이템별 추적 가능 및 다시 쓰기 가능 등 기존의 바코드 인식기술에 비하여 많은 장점으로 인하여 바코드 기술의 대체기술로 알려져 있다. 하지만 공간을 매개로한 전자파의 전달 특성은 전파되는 정보가 공간을 매개로 쉽게 노출될 수 있는 위험도 동시에 지니고 있어서 보안 및 프라이버시 문제가 항상 존재한다.

이 같은 RFID 보안 및 프라이버시 문제를 해결하기 위해 많은 연구가 활발하게 진행 되었으며, 크게는 물리적 접근 방법과 암호학적 접근 방법으로 분류할 수 있다. 물리적 접근 방법은 태그를 무효화시키는 Kill 명령어, Faraday Cage 기술, Blocker Tag 및 Active Jamming 기술 등의 방법이 있고, 암호학적 접근 방법으로는 비트연산(XOR), 재 암호화, 해쉬 함수 기반 및 전통적인 암호화(대칭키 및 공개키)기반 기법 등이 있다. 물리적 접근 방법은 Kill명령어와 같이 완벽하게 프라이버시를 보호할 수는 있는 것도 있으나 재사용을 못하게 하거나 추가적인 비용을 지불하는 등의 단점이 존재한다. 따라서 RFID 보안 및 프라이버시 보호 뿐 아니라 인증 및 데이터 보호까지 고려하기 위해서는 암호학적 접근 방법으로 해결해야 할 필요성이 있다. 암호학적 접근 방법 중 해쉬 함수 기반의 알고리즘은 일방향 해쉬 함수의 역함

† 정 회 원 : 경북대학교 BK21 Post-Doc
†† 준 회 원 : 경북대학교 전기전자컴퓨터공학부 석사과정
††† 정 회 원 : 대구가톨릭대학교 기초학부 강의전담 교수
†††† 정 회 원 : 경운대학교 컴퓨터공학과 교수
††††† 종신회원 : 경북대학교 컴퓨터공학과 교수

논문접수 : 2009년 8월 27일
수 정 일 : 1차 2009년 10월 25일
심사완료 : 2009년 11월 1일

수 계산 어려움에 기반하여 프라이버시, 추적 등의 보안 문제를 해결하기 위한 적합한 알고리즘이나 표준 SHA 계열의 해쉬 함수를 하드웨어로 구현하면 8천~만 게이트 이상이 소요된다. 따라서 현실적으로 수천 게이트 정도의 자원만 사용 가능한 RFID 태그에서는 구현하기에는 커다란 도전이 되고 있다. RFID 태그에 구현 가능한 초경량 해쉬 함수가 있다면 구현 가능한 기술로 Weis 등[1]이 제안한 Hash-lock 프로토콜로 인하여 이후에 RFID 인증 프로토콜의 많은 프로토콜들[2-4]이 초경량 해쉬 함수를 기반으로 하는 계기가 되었다. 이는 해쉬 함수의 역함수 계산의 어려움에 기인한 안전성 때문이다. 한편 공개키 기반 알고리즘은 키 분배 및 키 관리 문제를 고려할 때 적합한 암호 알고리즘으로, 최근에 Rabin, NTRU, ECC등의 공개키 기반으로 한 하드웨어 구현[5-6]에 활발한 연구가 이루어지고 있으나, 이 역시 해쉬 함수 기반과 같이 현실적으로 적용하기 어려움이 있다. 한편, 대칭키 암호 알고리즘은 최근 미국 표준 블록 암호 AES를 3,600 게이트 구현에 성공한 사례가 발표되었고[7], 또 SHA1과 같은 해쉬 함수보다 AES 대칭키 암호가 저전력 설계에 더 적합함이 다양한 논문을 통해 입증되었다. Feldhofer 등[8]의 최근 논문에서 대칭키 AES-128은 어떤 해쉬 함수 보다 더 RFID 시스템에 적합하다고 제안한 바 있다. 구본석 등[9]은 Feldhofer 등[7]보다 진일보한 암·복호화가 가능한 초소형 AES 연산기를 3,992 게이트로 구현한 바 있다. AES 외에도 mCrtton[10], HIGHT[11] 및 PRESENT[12] 등의 경량화 블록 암호화(대칭키 암호)시스템이 3,000 게이트 이하에서 구현됨으로 자원제약이 심한 저가(Low-cost)의 RFID 태그에 여유 있게 적용될 수 있음을 알 수 있다. 한편 Osaka 등[4]은 RFID 시스템의 소유권 이전 기법에 해쉬 함수와 대칭키 암호시스템을 병행하여 사용하여, 인증 시에는 해쉬 함수를, 그리고 키 이전 시에는 대칭키 암호기법을 활용하는 예를 보여 주었다. 최근에 Toiruul 등[13]은 랜덤 비밀키 k_1, k_2을 데이터베이스와 태그가 공유하는 대칭키 AES를 이용한 상호인증 기법을 제시한 바 있다. 위와 같은 하드웨어 구현의 진일보된 연구에도 불구하고 대칭키 인증 방식의 취약점은 해당 서비스에 속해 있는 모든 태그들이 동일한 암호키 K를 사용하여 보안을 수행한다는 점이다. 즉 하나의 태그로부터 키가 공개될 확률은 적지만 만약 공유된 키가 하나라도 노출이 된다면[14] 다른 모든 태그의 정보가 무력화되는 위험성을 내포하고 있다. 키가 노출될 수 있는 경로는 키 관리자가 악의적으로 노출할 경우와 물리적 공격(예 : 탐사공격)에 의해 노출될 가능성이 있다. 후자의 경우 방지대책은 PUF(Physically Unclonable Function)를 활용하여 태그의 복제를 방지하는 방법으로 가능하며, 이에 대한 연구가 활발히 진행되고 있다.[15-16] Tuyls 등[17]은 RFID 태그의 복제방지를 위해서 PUF 및 공개키 암호를 사용하여 인증 프로토콜을 제안한 바 있고, 최근 Kulseng 등[18-19]은 RFID 경량 검색 프로토콜에서 PUF 및 LFSR을 활용함으로 태그의 경량화를 증진시켰다.

본 논문에서는 대칭키 노출에 대한 위험을 차단할 수 있는 방안을 제시함으로 대칭키 암호기법 자체가 가지고 있는 구현 용이성을 충분히 활용하고자 한다. 안전한 RFID 인증 프로토콜을 설계하기 위하여 리더와 태그가 상호인증 가능해야 하고 위치추적을 피할 수 있어야 함을 Choi 등[20]등은 제시한 바 있다. 여기에 최근의 인증프로토콜의 경향을 보면, 태그와 리더 간에 교환되는 메시지를 보호하기 위해 난수생성기를 적극 활용하고[21], RFID 시스템의 보다 경량화된 인증기법[22]을 도입하며, 최소한의 암호학적 접근 방식[23] 등을 활용함을 알 수 있다.

위와 같은 기준을 기반으로 본 논문에서는 저가의 상호인증가능하며 난수발생기를 적극 활용하고, 최소한의 암호화 접근 방식을 도입하는 등의 설계기준에 따라 대칭키와 해쉬 함수를 병행하여 사용하는 상호인증방식을 제안한다. 제안한 프로토콜은 태그에 구현하기 용이한 대칭키를 인증프로토콜로 사용함으로 해쉬 함수나 공개 키 알고리즘보다 하드웨어 자원을 줄일 수 있고, 태그 ID를 일 방향 함수의 역함수 계산 어려움에 기반 한 해쉬 함수로 암호화하여 사용함으로 물리적인 탐사 공격 시에 예상되는 태그 ID 노출을 차단할 수 있다.

또한 제안한 프로토콜은 기존의 대칭키 암호 기법처럼 사전에 대칭키를 미리 공유하지 않고, 배선의 전기적 특성이 칩 별로 다르다는 점을 활용한 IC칩의 고유한 지연특성을 갖는 PUF(Physically Unclonable Function)의 입출력인 Challenge-Response 값을 공유 대칭키로 활용하기 때문에 키 노출 위험이 없는 안전한 프로토콜이며, 설령 키가 노출된다 해도 해당 세션마다 키가 바뀌기 때문에 다른 태그에 영향이 없는 안전한 프로토콜이다. 그리고 효율적 측면에서도 최근에 제안된 기법[13]과 비교해 볼 때 결코 뒤지지 않는 우수한 효율성을 보임을 알 수 있다.

본 논문의 구성은 기존의 먼저 인증 프로토콜을 분석한 후, 대칭키, 해쉬 함수 및 PUF를 활용한 RFID 인증 프로토콜을 제시한 후, 제시한 프로토콜이 예상 공격에 안전함을 논리적으로 분석하여 서술하고, 효율성(Efficiency) 분석을 한 후 마지막으로 결론을 맺는다.

2. RFID 시스템

2.1 RFID 시스템의 구성

RFID기술 시스템은 태그, 리더 및 데이터베이스로 구성되며, 각각의 기능은 다음과 같다.

2.1.1 태그

현재 RFID 시스템에 사용되는 태그는 반도체 칩과 안테나로 구성되며, 자체 전원을 사용하는 여부에 따라 수동형 및 능동형 등으로 나눌 수 있다. 수동형 태그는 리더에서 수신한 전파로부터 유도된 전류를 전원으로 사용하여 태그를 활성화하고 저장 데이터를 리더로 송신하는 역할을 한다.

2.1.2 리더

RFID 리더는 일반적으로 RF모듈, 제어 유닛 그리고 라디오 주파수 교환을 통해 전자 태그에 신호를 전달하는 연결 장치로 구성된다. 리더는 태그에 비해 더 큰 저장 공간과 더 좋은 처리 능력을 가지며, 데이터베이스에 연결할 수 있다. 리더는 태그에 무선을 사용하여 정보를 요청하고 받는다.

2.1.3 데이터베이스

데이터베이스는 태그에 관련된 정보를 저장하고 관리하는 역할을 한다. 이것은 태그에 저장되는 정보를 적은 비트로 제한하여 처리능력과 저장능력의 제약을 극복하려는 의도이다. 처리 속도와 저장 공간에 대한 제약이 크지 않아 일반적으로 리더와 데이터베이스간의 연결은 안전하다고 가정한다.

2.2 RFID시스템의 안전성 조건

RFID 시스템의 안정성을 보장할 수 있는 조건은 아래와 같다.

2.2.1 도청(Eavesdropping)

RFID 시스템의 태그와 리더간은 무선을 전제로 하고 있기 때문에 공격자는 리더와 태그 사이에 전송되는 메시지를 도청할 수 있다. 공격자는 도청을 통하여 사용자의 비밀 정보를 얻거나, 도청된 메시지를 이용하여 여러 가지 공격에 활용 할 수 있다.

2.2.2 재전송 공격(Replay Attack)

공격자는 도청을 통하여 태그에서 전송하는 고유 정보를 얻는다. 그 이후 리더의 요청에 대해 공격자는 정상 태그를 대신하여 자신이 이전에 도청을 통하여 얻었던 정보로 응답한다. 따라서 공격자는 정상인 태그인척 위장하여 정상리더를 속일 수 있다.

2.2.3 위치 추적(Location Traceability)

사용자가 태그가 부착된 상품을 소지하고 있다면 태그의 고유 식별 정보를 통하여 사용자와 연관성을 줄 수 있다. 따라서 공격자는 사용자가 소지한 특정 상품의 도청을 통하여 이동경로를 추적하여 프라이버시를 침해할 수 있다.

2.2.4 상호인증(Mutual Authentication)

리더(또는 태그)가 태그(또는 리더)를 동시에 서로를 정당한 개체라고 확신하는 과정을 말하며, 이와 같은 과정이 없을 때 공격자는 리더나 태그에 대해 위조할 수 있게 된다.

2.2.5 대칭키 K의 노출에 따른 위험

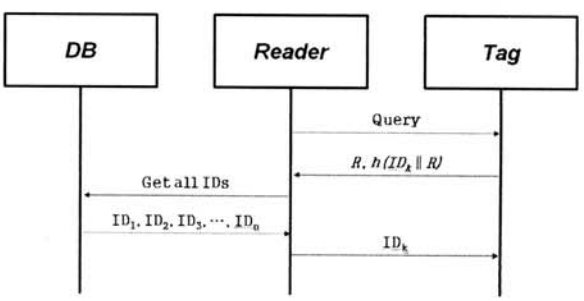
대칭키 암호 시스템은 동일하게 공유하는 대칭키 K를 사용하여 보안을 수행하는 프로토콜로써 만약에 키가 노출된다면 이에 따른 다른 모든 태그의 정보를 무력화시키는 위험성이 있다. 예상되는 키 노출 경로는 악의적으로 대칭키 K를 적에게 넘겨주는 경우와 물리적 공격인 탐사공격(Probe Attacks)에 의해서 야기될 수 있다.

3. 관련연구

지금까지 많은 프로토콜이 제시가 되었다. 실제로 EPC CLASS 0, 1 수동형 태그의 경우 읽기 전용으로 복잡한 로직을 수용할 수는 없는 한계점이 있다. Weis 등[1]은 수동형 RFID 설계 시에 전체 500~5000 게이트로 구성될 것으로 추정하였다. 그리고 EPC CLASS 2의 경우 역시 수동형 태그이며 다시쓰기 가능한 메모리 및 추가적인 하드웨어 자원을 가지고 있어 약 10,000 게이트 정도로 구성될 것으로 보고 있다[24]. 본 논문에서는 현실적으로 저가형 태그에 구현하기에 가장 용이하면서 안전한 프로토콜을 설계하는데 초점을 맞춘다. 이를 위해 먼저 기존의 인증 프로토콜을 분석한다.

(그림 1)은 Weis 등[1]이 제안한 Randomized Hash Lock 프로토콜을 보여준다.

Weis 등[1]이 보안과 프라이버시 문제를 표준적인 RFID 태그의 범주보다 더 넓은 영역 안에서 태그에 하드웨어적으로 최적화되어 구현 가능한 초경량 해쉬 함수가 있으면 구현 가능한 기술로서 제시한 Hash-lock 프로토콜은 일방향 해쉬 함수의 역함수를 구하는 어려움에 기반하여 인가되지 않은 리더가 태그의 내용을 읽어내는 것을 방지하는 기법이나, 사용자가 위치 추적될 수 있는 문제를 해결하지 못하는 단점이 있었다. 그들은 Hash-lock 방법을 좀 더 확장하여 Randomized Hash Lock(①) 알고리즘을 제안하였다. 이 방법은 적은 태그를 소유한 경우에 적합하며 앞서 제안한 해쉬-락 기법에서 위치추적을 피하기 위해, 태그는 해쉬 함수 이외에 의사난수생성기가 기본적으로 있다고 가정하고, 위치 추적에 안전한 프로토콜을 설계하였지만 리더에서 모든 ID에 대하여 해쉬 함수를 계산하기 때문에 리더에 과도한 부하가 걸린다. 또한 상호인증을 고려하지 않고 설계하였기 때문에 도청을 통하여 태그가 보내는 값을 저장하였다가 리더의 질의에 응답하여 정당한 태그인 척 위장하여 기존의 저장한 값을 리더에게 전송함으로써 리더를 속일 수 있다. 따라서 재전송 공격에 취약점이 있고 도청한 값을 이용하여 다른 공격에 이용이 가능하므로 도청에도 안전하다

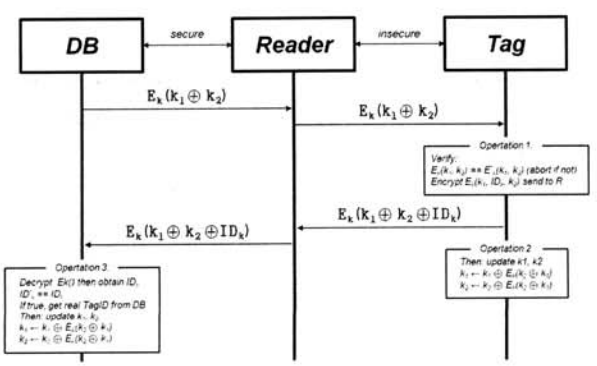


(그림 1) Randomized Hash Lock

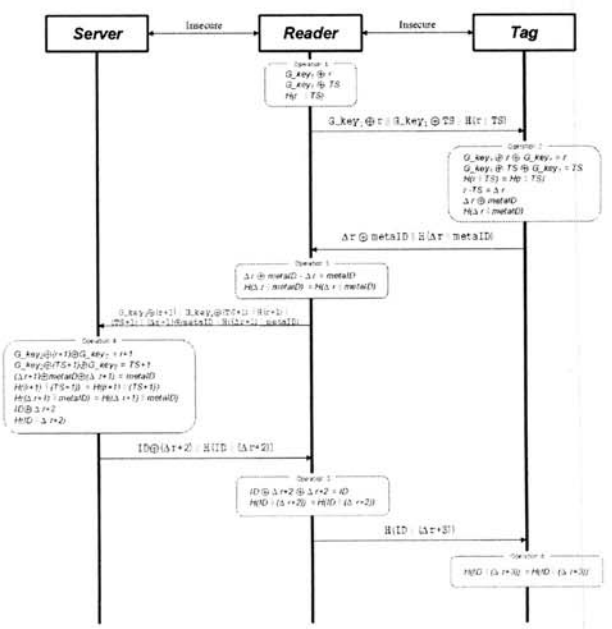
고 할 수 없다.

Toiruul 등[13]은 An Advanced Mutual-Authentication Algorithn Using AES 프로토콜(②)에서 대칭키 AES를 이용한 상호 인증기법을 제시하였다. (그림 2)는 Toiruul 등이 제안한 프로토콜에 대해 보여준다. 이 기법에서 리더 R의 역할은 중계자 역할을 담당하고, 주로 데이터베이스 B와 태그 T 간에 인증을 담당하는 구조이다. 먼저 B에서 질의에 해당하는 $E_K(k_1 \oplus k_2)$ 값을 R을 향해 날리면 R은 T에게 이 값을 보낸다. 여기서 K는 B와T만 알고 있는 암호키이며, $k_1.k_2$값은 B와 T만 알고 있는 랜덤 비밀키이다. 태그에서는 자신이 알고 있는 랜덤 비밀키 $k_1.k_2$을 암호화하여 R에게 받은 값과 일치하는지 확인하여 R을 인증한다. 다음 T는 B와 T만이 알고 있는 자신의 ID_K값과 $k_1.k_2$을 XOR하여 $E_K(k_1 \oplus k_2 \oplus ID_K)$을 R에게 보낸 후 자신의 랜덤 비밀키 $k_1.k_2$를 갱신한다. R은 이 값을 중계하여 B에게 보내면 B에서는 이 값을 복호화하여 $ID^*_K \equiv ID_K$이면 태그의 정당성을 인증하고, 자신의 랜덤 비밀키 $k_1.k_2$ 값을 갱신한다. 제안된 프로토콜에서는 $E_K(k_1 \oplus k_2)$ 값을 도청하여 저장한 후 재전송 공격을 하여도 태그는 이미 랜덤 비밀키 값들을 갱신한 상태이므로 [operation 1]에서 위조된 리더로부터 온 메시지인지를 판단 할 수 있다. 위치추적 문제도 [operation 2]에서 랜덤 비밀키 값을 갱신하기 때문에 $E_K(k_1 \oplus k_2)$ 값을 도청하여도 태그의 응답은 항상 변하기 때문에 위치 추적 문제를 해결할 수 있다. 또한 도청을 통하여 저장된 $E_K(k_1 \oplus k_2)$ 값을 재전송하여 위치추적을 시도하여도 [operation 1]에서 검증 후 부정당한 리더로부터 오는 메시지를 차단하여 태그로부터의 응답을 더 이상 받지 못하게 되어 위치추적 문제에 안전하다. 따라서 도청한 값을 다른 공격에 활용할 수 없으므로 도청에 안전하고 위치추적 및 재전송 공격에 안전한 프로토콜이다. 하지만 제안한 프로토콜에서는 초기 대칭키와 랜덤 비밀키가 알려지게 되면 프로토콜 전체에 영향을 미치게 되어 안전하지 못하게 된다. 또한 제안된 프로토콜에서는 랜덤 비밀키를 어떻게 B와 동기화 할 수 있을지가 관건이다.[25] 즉, B와 T가 랜덤 비밀키 $k_1.k_2$를 갱신하는데 서버와 동기화가 이루어지지 않는 태그는 정당한 태그라 할지라도 더 이상 사용할 수 없게 되는 문제점이 발생할 수 있다.

Kang 등[26]은 A study on secure RFID mutual authentication scheme in pervasive computing environment 프로토콜(③)에서 Hash함수를 이용한 상호 인증기법을 제시하였다. (그림 3)은 Kang 등이 제안한 첫 번째 프로토콜에 대해 보여준다. 제안한 논문에서는 기존 논문과 다르게 고정형 리더가 아닌 이동식 리더로 가정하였다. 즉, 리더와 태그 사이는 물론 리더와 서버사이도 안전하지 않은 채널에서의 서버와 리더, 서버와 태그, 리더와 태그 간에 상호인증 프로토콜을 제안하였다. 제안한 상호인증 프로토콜에서 G_key1은 리더와 태그 사이의 공유키이고 G_Key2는 리더와 서버 사이의 공유키로써 사전에 안전한 채널을 통하여 키를 저장한다. 또한 이 기법은 서버에서 △r을 계산해야 하므로 리더에서 생성한 r, TS가 중요 역할을 한다. 상호인증 과정은 [Operation 2]에서 r, TS를 G_Key1을 통해 얻어내고 해쉬 함수를 통하여 r, TS가 정당한 리더에서 온 것인지를 판단하여 태그는 리더가 정당한지를 인증한다. [Operation3]에서는 △r을 통하여 metaID 값(metaID가 유효한지는 Operation 4과정을 통하여 확인)을 얻어내고 해쉬 함수를 통하여 △r, metatID가 정당한 태그에서 온 것인지를 판단하여 리더는 태그가 정당한지를 인증하는 과정이다. 제안한 프로토콜에서는 서버와 리더 사이도 안전하지 못한 채널이라고 가정하였다. 따라서 [Operation4]에서 G_Key2를 통하여 r+1, TS+1값을 얻은 후, 각각 -1을 행한다. 그 후 r, TS를 얻은 후 r-TS를 통하여 △r를 얻는다. 그리고 metaID에 해당하는 ID가 있는지를 검색 후 metaID가 정당한지를 확인한다. 또한 해쉬 함수를 통하여 r+1, TS+1값이 정당한 리더에서 온 것인지를 판단하여 서버가 리더가 정당



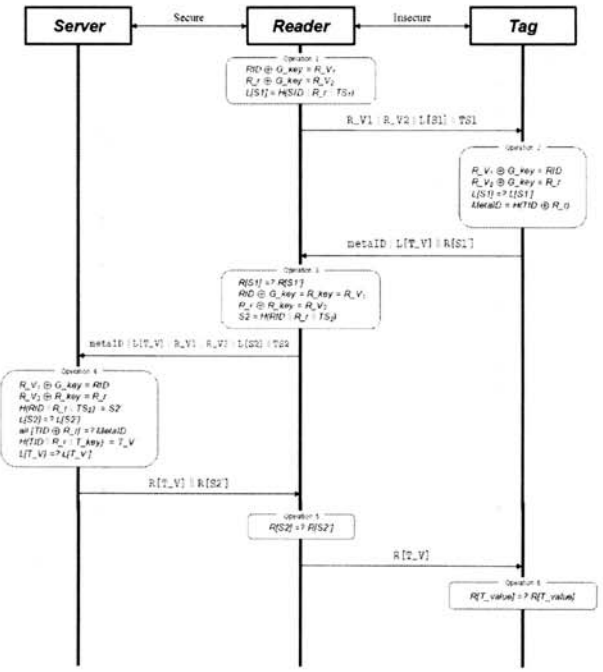
(그림 2) Advanced Mutual Authentication Protocol



(그림 3) Secure RFID mutual authentication scheme(Protocol I)

한지를 인증한다. [Operation 5]에서 △r+2를 통하여 ID(ID가 유효한지는 Operation 6을 통하여)를 얻는다. 만약에 리더가 전송한 r, TS가 정상적인 통신을 통하여 전송되지 않았다면 △r+2 또한 정상적이지 않기 때문에 해쉬 함수를 통하여 서버가 정당한지를 확인한다. [Operation 6]에서 해쉬 함수를 통하여 정당한 리더에서 온 것인지를 확인하고 또한 ID를 통하여 정당한 서버로부터 온 메시지인지를 판별 가능하다. 제안한 프로토콜에서는 서버와 리더, 서버와 태그, 리더와 태그 간에 상호간의 인증이 가능하다. 하지만 제안한 논문에서는 위치추적 및 재전송 공격에 취약점을 보인다. 첫 번째 단계를 도청하여 부정당한 리더가 태그에게 전송할 경우 태그는 리더에서 전송한 랜덤 값을 기반으로 하여 연산하기 때문에 동일한 값을 전송한다. 따라서 위치 추적문제를 완전히 해결했다고 볼 수 없다. 제안한 프로토콜에서 재전송 공격의 경우 상호인증을 통하여 서버, 리더, 태그에서 위조된 객체들을 판별할 수 있기 때문에 안전하다. 하지만 위치추적과 마찬가지로 항상 동일한 값을 전송하는 것은 재전송 공격에 대해 완벽하게 안전하다고 할 수 없다. 즉, 첫 번째 단계를 도청을 통하여 저장하고 있다가 정당한 리더인척 위장하여 태그에게 전송하면 태그는 항상 동일한 값을 전송하므로 안전성에 문제가 발생한다. 또한 제안한 프로토콜에서 가장 큰 문제점은 G_Key라는 정보를 모든 태그가 동일하게 가지고 있어야 하는 문제점이 있다. 가정 사항에 안전한 채널에서 G_Key값을 서로 공유하였다 하더라도 프로토콜에서 G_Key값이 노출되게 되면 하나의 태그가 아니라 전체 시스템의 안전성에 영향을 미칠 수 있다. 따라서 제안한 프로토콜은 언제 노출될지 모르는 고정된 G_Key값을 프로토콜에서 사용해야 하는 문제점을 계속 가지고 가야 할 것이다.

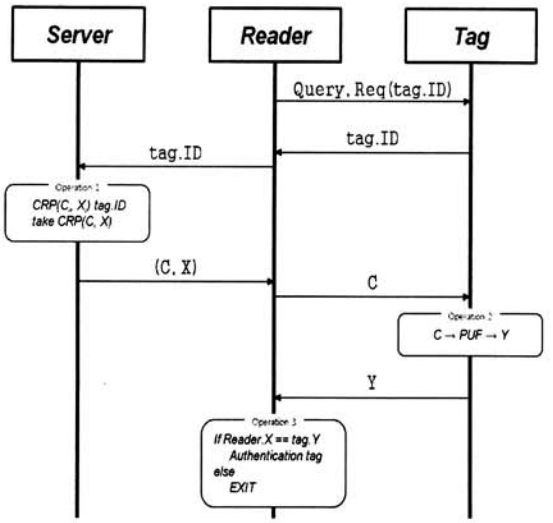
Kang 등은 [26]에서 태그의 연산량을 줄이기 위해 두 번째 프로토콜(④)을 제시하였으며, (그림 4)는 두 번째로 제안한 프로토콜을 보여주고 있다. 두 번째 프로토콜 역시 해쉬 함수 기반이며 리더와 태그 사이, 리더와 서버사이 모두 안전하지 않은 채널에서 서로 간에 상호인증 프로토콜을 제안하였다. 제안한 프로토콜에서 G_Key는 서버, 리더, 태그가 안전한 채널에서 공유한 키이며 R_Key(리더의 고유한 키)는 서버와 리더 사이에 공유한 키이고 T_Key는 태그의 고유한 키이다. 또한 TS1은 리더와 태그사이에서 사용하는 타임스탬프이고, TS2는 리더와 서버사이에서 사용하는 타임스탬프이다. 제안한 프로토콜에서 상호인증 단계는 [Operation 2]에서 G_Key를 통하여 RID, R_r값을 얻은 후 전송된 TS 값을 이용하여 L[SI](H(RID||R_r||TS)값의 왼쪽에서 반값)을 생성하고 리더에서 전송받은 값과 비교하여 같은지를 비교한다. 값이 같다면 태그는 정당한 리더로부터 온 메시지인지를 판단 할 수 있다. 리더에서 태그를 인증한다. 값이 같다면 태그는 정당한 리더로부터 온 메시지인지를 판단 할 수 있다. 리더에서 태그를 인증하는 과정은 [Operation 3]에서 R[SI](H(RID||R_r||TS)값의 오른쪽에서 반값)을 생성하고 태그에서 전송받은 값과 같은지를 비교하여 값이 같다면 정



(그림 4) Secure RFID mutual authentication scheme (Protocol II)

당한 태그로부터 온 것인지를 판단 할 수 있다. [Operation 4]에서는 G_Key와 R_Key를 이용하여 RID, R_r을 얻은 후 전송된 TS2값을 이용하여 L[S2]값을 생성한다. 생성한 값과 리더에서 전송 받은 값이 같다면 서버는 정당한 리더로부터 메시지가 전송된 것인지를 판단할 수 있다. 또한 서버는 태그의 TID와 T_Key를 얻기 위해 metaID(H(TIDxorR_r)와 일치하는 모든 TID에 대하여 계산 후 TID, T_Key를 얻는다. 그 후 L[T_V]를 생성한 후 리더에서 전송한 L[T_V]와 같은지를 계산하여 같다면 정당한 태그로부터 온 것인지를 판단할 수 있다. [Operation 5]에서 R[S2]를 생성하여 서버에서 전송받은 값과 같은지를 비교한다. 그 후 같다면 리더는 정당한 서버로부터 온 메시지라는 것을 판단할 수 있다. [Operation 6]에서 R[T_Value]를 생성한 후 리더에서 전송받은 R[T_V]와 비교하여 같은지를 체크하고 같다면 태그는 정당한 서버임을 확인한다. 제안한 프로토콜은 태그에서의 연산량을 줄이는 반면에 서버의 연산량을 O(N)만큼 수행해야 한다. 또한 제안한 첫 번째 프로토콜과 마찬가지로 리더에서 전송하는 값을 이용하여 태그에서 연산을 한 후 리더로 전송하기 때문에 위치추적 및 재전송 공격에 취약점을 보이며 고정된 G_Key값을 사용하므로 G_Key값 노출 시 전체 시스템이 정상적으로 동작하지 못하는 문제점이 발생한다.

Tuyls 등[17]은 복제방지를 위한 RFID 태그를 위해서 PUF 및 공개키 암호를 사용하여 인증프로토콜을 제안한 바 있다. [17]에서는 PUF만을 사용하여 리더가 태그를 인증하는 단방향 인증프로토콜과 PUF 및 공개키 암호화를 이용한 인증 프로토콜을 제안하였다. PUF와 공개키 암호화를 이용한 인증 프로토콜에서는 태그가 먼저 리더에게 요청하는 과



(그림 5) PUFs and Public-Key Cryptography for RFID-Tags

정으로부터 통신을 시작하므로 일반적인 RFID 시스템에서의 통신(수동형 RFID 태그)이라고 볼 수 없다. 따라서 본 장에서는 PUF만을 이용한 인증 프로토콜에 대해서 언급한다. (그림 5)는 제안한 프로토콜 중에서 PUF만 이용한 인증 프로토콜에 대해 보여주고 있다.

인증 단계의 시작은 리더가 태그에게 Query와 함께 태그의 ID를 요청하는 것으로 시작한다. Query를 받은 태그는 자신의 ID를 리더에게 전송하고 리더는 서버에게 ID를 전송하여 ID에 해당하는 $CRP_i(C_i,X_i)$ 쌍 중에서 하나를 DB로부터 전송 받는다. 리더는 전송받은 C, X 중에서 C 값을 태그에게 전송한다. C 값을 전송받은 태그는 PUF를 통하여 C에 해당하는 값인 Y를 출력하여 리더에게 전송한다. 리더는 서버에서 받은 X값과 태그에서 받은 Y값이 같은지를 확인하여 같으면 태그를 인증한다. [17]에서는 PUF를 통하여 리더에서 태그가 정당한지를 확인하는 단방향 인증 프로토콜로써 태그의 복제 여부를 확인할 수 있지만 도청, 위치추적, 재전송 공격에 안전하지 못하다. 위치 추적의 경우 리더에서 Query값을 보내면 항상 동일한 Tag의 ID를 보내고, 도청하여 얻은 C의 값에 의해 태그는 항상 동일한 Y값을 전송하기 때문에 안전하지 못하다. 재전송 공격의 경우 위치추적의 문제와 같은 관점으로 고정된 값을 전송하는 것과 단방향 인증 프로토콜에 의해 태그는 리더를 인증하지 못한다. 따라서 공격자는 정당한 리더인척 위장하여 태그를 속일 수 있다. 또한 도청을 통하여 얻은 값을 다른 공격에 활용 가능 하므로 도청에도 취약하다.

4. 제안 상호 인증 프로토콜

지금까지의 보안 및 프라이버시 인증 기법을 분석한 결과를 토대로 RFID 보안 및 프라이버시 문제로부터 안전한 인증 프로토콜을 설계한다.

제안한 프로토콜에서 사용되는 표기법은 <표 1>과 같다.

〈표 1〉 표기법

기 호	정 의
Rr_i	리더에서 생성한 랜덤 값
Rt_i	태그에서 생성한 랜덤 값
ID_i	태그의 ID
ID_p	태그의 PUF(Physically Unclonable Function) ID
$_{prev}ID_p$	태그의 이전(previous) PUF ID
$IDinfoi$	태그 ID의 정보(information)
$H(x)$	일방향 해쉬 함수, SHA-1
$H(ID)$	태그 ID을 해쉬 함수로 암호화한 값
EX	대칭키 알고리즘, AES-128로 암호화
DX	대칭키 알고리즘, AES-128로 복호화
$CRP_i(C_i,X_i)$	ID_p에 대한 Challenge -Response Pairs, 즉 challenge C_i에 값에 대한 response X_i값의 쌍 집합. X_i값이 공유 대칭키가 됨.
$\|$	연접(concatenation), 연결

4.1 가정사항

(1) 태그는 리더에서 전원을 받아 동작하는 수동형 태그이다.

(2) 리더와 태그 간에는 공격자가 시스템에 공격을 가할 수 있으나, 리더와 데이터베이스 간에는 공격에 안전하다고 가정한다.

(3) 리더와 태그는 AES-128 대칭키 알고리즘, 의사난수 발생기 및 XOR연산을 수행할 수 있다.(M. Feldhofer 등[7]이 전력소모와 소자면적을 최소로 하기 위하여 단방향 인증의 설계를 AES 암호화만 이용하여 구현하였으나, 구본석 등[9]은 암·복호화가 가능한 연산기를 구현하여 실제로 태그의 암·복호화가 가능함을 보였다.)

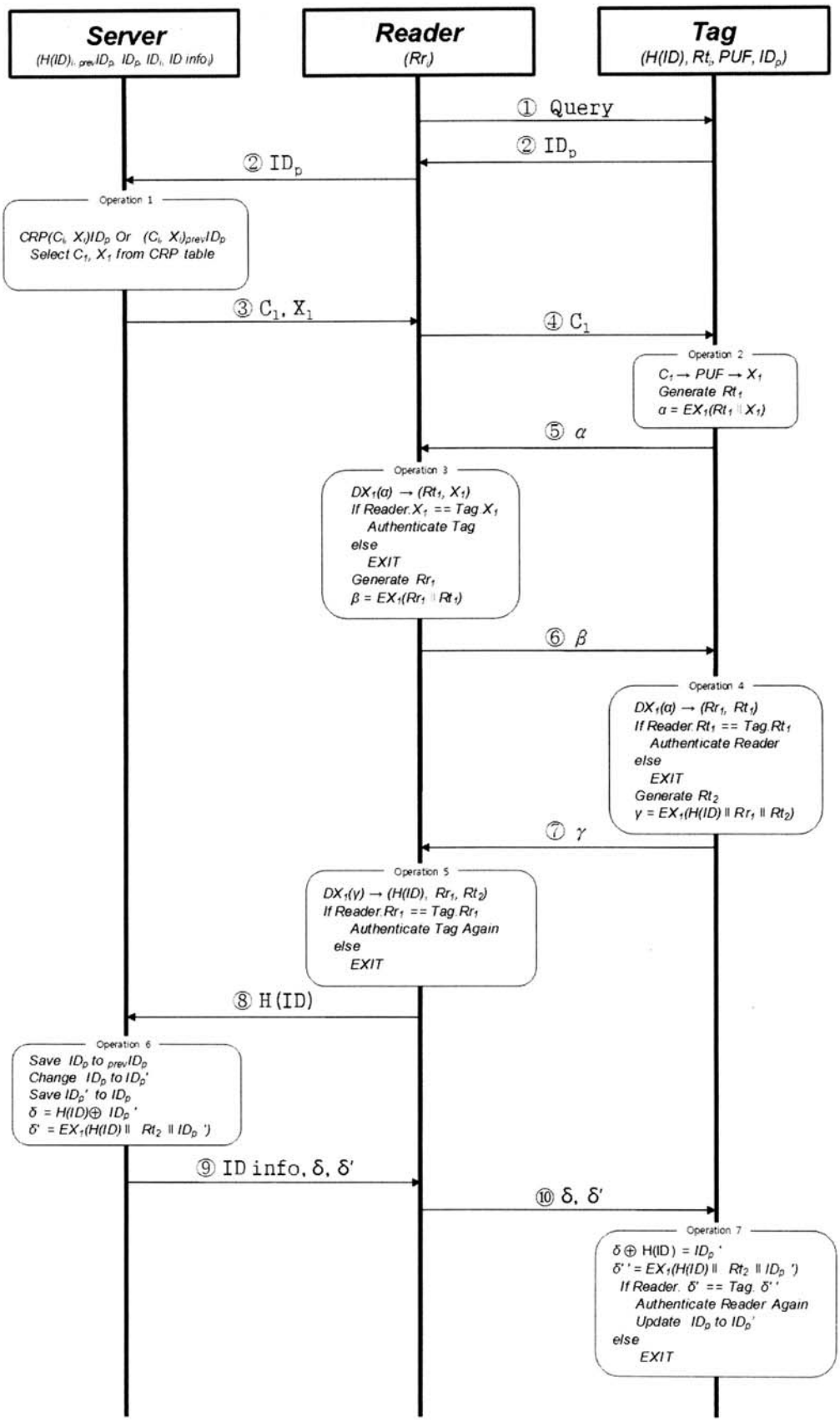
(4) 태그에는 128-bit PUF가 설치되어 있다고 가정한다.

4.2 초기 단계

초기 단계에서는 태그 제조자는 각 태그마다 태그 ID를 일방향 해쉬 함수(SHA-1) $H(x)$로 암호화한 값 $H(ID)$와 PUF의 ID 즉 ID_p를 태그에 저장한다. 또한 데이터베이스에는 태그ID와 $H(ID)$에 대한 테이블 $ID_i - H(ID_i)$ 및 PUF에 대한 입력값 C_i와 이 입력값에 대한 출력값 X_i의 CRP(Challenge -Response Pair) 테이블 $CRP_i(C_i,X_i)$를 만들어 저장한다.

4.3 인증 프로토콜

태그와 리더는 다음과 같은 절차를 통해 서로를 인증한다. (그림 6)은 제안한 상호인증 프로토콜을 보여주고 있다. 전체 프로토콜을 먼저 PUF를 이용하여 공유 대칭키(shared symmetric key)를 취득하는 과정과 공유 대칭키를 얻고 난 다음 이 공유 대칭키로 리더와 태그 간에 상호 인증을 수행하는 과정으로 크게 나눌 수 있다.



(그림 6) 제안한 상호인증 프로토콜

step 1 (질의) 수동형 RFID 태그는 자체전원 없이 리더로부터 수신한 전자기파에 의해 유도된 전류를 전원으로 사용하고, 리더의 Query가 있어야 이에 반응하여 통신할 수 있다. 리더는 태그의 전송 데이터를 인식하기 위하여 주기적으로 Query를 보낸다.

step 2 (ID_p 전송) 리더가 전송하는 Query 신호에 의해 태그는 전원을 공급받고 리더의 요청에 응하는 값 즉 태그의 PUF ID, ID_p를 리더에게 보낸다. 리더는 이 값을 그대로 DB에 전송한다.

step 3 (CRP전송) 리더로부터 PUF ID, 즉 ID_p를 받은 DB는 해당 PUF의 Challenge-Response 쌍 집합인 $CRP_i(C_i,X_i)$에서 하나의 값 $CRP_1(C_1,X_1)$을 선택하여 그 값을 리더로 보낸다. 이때 ID_p가 갱신된 값이면 ID_p값을 갱신되지 않은 값이면 $_{prev}ID_p$값을 사용하게 된다.

step 4 (Challenge C_i 전송) DB에서 $CRP_1(C_1,X_1)$를 받은 리더는 Challenge C_1값만을 태그로 전송한다.

step 5 (공유 대칭키 획득) 리더에서 Challenge C_1값을 받은 태그는 이 값을 PUF에 입력하여 출력값 X_1를 얻고 이 값을 리더와 태그 사이의 공유 대칭키로 사용한다.(리더는 DB에서 얻은 $CRP_1(C_1,X_1)$에서 Response X_1값을 이미 알고 있다.) 또한 태그 내에 있는 난수 생성기를 통하여 생성된 랜덤 값 Rt_1과 X_1을 연접한 후 AES-128 대칭키 알고리즘(공유 대칭키X_1)으로 암호화하여 이 값(α)을 리더에게 전송한다.

step 6 (태그 인증 및 β값 송부) 리더는 α값을 AES-128 대칭키 알고리즘(공유 대칭키X_1)으로 복호화한 값 $Rt_1 \| X_1$ 중에서 X_1값을 취하여 $CRP_1(C_1,X_1)$의 X_1값과 일치하는지 않는지를 확인하고, 일치하면 태그가 정당한 태그임을 인증한다. 만약 태그에서 보내온 X_1과 $CRP_1(C_1,X_1)$의 X_1과 일치하지 않으면 불법한 tag임으로 세션을 끝낸다. 인증된 태그일 경우 리더는 랜덤 값 Rr_1을 생성한 후 태그가 보내준 Rt_1과 연접한 후 공유 대칭키X_1으로 암호화 하여, 이 값(β)을 태그로 전송한다.

step 7 (리더 인증 및 $H(ID)$송부) 태그는 리더에서 받은 값 β를 AES-128 대칭키 알고리즘으로(공유 대칭키X_1)으로 복호화하여, 리더에서 얻은 값Rt_1과 태그가 발생한 Rt_1이 동일하면 정당한 리더임을 인증한다. 만약 일치하지 않으면, 세션을 끝낸다. 정당한 리더일 경우, $H(ID)$값과 랜덤 값 Rr_1과 새로 태그에서 생성한 랜덤값 Rt_2를 서로 연접한 후 이를 공유 대칭키X_1으로 암호화하여 리더에게 이 값(γ)을 전송한다.

step 8 (ID info 값 조회) 리더는 γ값을 AES-128 대칭키 알고리즘(공유 대칭키X_1)으로 복호화한 값 $H(ID)\|Rr_1\|Rt_2$ 중에서 Rr_1을 취하여 리더에서 생성한 값과 비교하여 동일하면, 정당한 태그임을 다시 검증하고 $H(ID)$ 값을 서버에게 보낸다.

step 9 (ID info, δ, δ' 전달) 서버는 $H(ID_i)-ID_i$ 테이블에서 ID_1값에 대한 정보 ID_{infoi}를 찾는다. 그리고 $CRP_1(C_1,X_1)$에서 (C_1,X_1)을 제거한다. 서버는 ID_p값을 갱신하기위하여 이 값을 $_{prev}ID_p$에 저장한 후 ID_p를 ID_p'로 바꾸고 이 값을 ID_p에 저장한다. δ, δ'을 계산하여 ID_{infoi}과 함께 리더로 보낸다.

$$\delta = H(ID) \oplus ID_p'$$
$$\delta' = EX_1(H(ID)\|Rt_2\|ID_p')$$

step 10 (ID_p값 갱신) 리더는 δ, δ'을 태그로 보내면, 태그는 δ값을 $H(ID)$을 XOR하여 ID_p'을 얻고, 또 $H(ID)$과 Rt_2과 ID_p'를 서로 연접하여 공유 대칭키X_1으로 암호화하여 δ''를 얻는다.

$$\delta \oplus H(ID) = ID_p'$$
$$\delta'' = EX_1(H(ID)\|Rt_2\|ID_p')$$

이때 계산한 값 δ''과 δ'값이 같으면 태그는 리더를 다시 한번 검증한 후, 정당한 리더임으로 태그의 ID_p값을 ID_p'으로 갱신한다. 이로써 한 세션을 끝낸다.

5. 안전성 분석

본 장에서는 다양한 공격유형에 대하여 제안한 인증 프로토콜의 안전성에 대하여 기술한다. 그리고 기존에 제안된 프로토콜과 비교 분석한다.

5.1 공격유형에 따른 보안 분석

5.1.1 도청(Eavesdropping)

가정 사항에서 서버와 리더사이는 안전한 채널이고 리더와 태그사이는 안전하지 못한 채널이라고 가정하였다. 따라서 리더와 태그사이의 모든 단계에서 도청이 가능하다. 하지만 제안한 프로토콜에 의해 매 세션마다 항상 다른 값을 전송하기 때문에 공격자가 도청을 하여 얻은 정보만으로는 값을 유추하거나 다른 공격에 활용할 수 없다.

5.1.2 재전송 공격(Replay Attack)

공격자는 리더와 태그 사이에 전송되는 데이터를 도청하여 저장하고 있다가 정당한 태그나 리더인척 위장하여 그 메시지를 재전송하여 리더나 태그가 전송하는 특정 값을 얻을 수 있다. 재전송 공격을 방지하기 위해서는 리더와 태그는 고정된 값을 전송하면 안 되며 리더와 태그 간에 상호인증이 되어야 한다. 제안한 프로토콜에서는 ID_p값은 프로토콜이 종료될 때마다 갱신되며 PUF의 출력 값을 키 값으로 사용하기 때문에 키 값이 일정하지 않고 매 세션마다 난수값을 포함한 정보를 암호화하므로 태그와 리더 사이에서 고정된 값이 출력되지 않는다. 또한 제안한 프로토콜은 리더와 태그 간에 상호인증을 한다. 따라서 제안한 프로토콜은 재전송 공격에 안전하다.(ID_p값이 업데이트 되지 않을 경우에 공격자가 기존에 저장해 놓은 ID_p값을 전송 시 $_{prev}ID_p$ 값에 해당하는 $CRP_1(C_1,X_1)$값을 보낸다. 하지만 C1값에 해당하는 X1값은 변하므로 기존에 저장해놓은 C1에 해당하는 X1값과는 다르다. 따라서 operation 3에서 태그 인증 시에 불법적인 방법으로 접근했다는 것을 알 수 있다.)

5.1.3 위치추적(Location Traceability)

태그가 리더에게 보내는 값이 고정되어 있는 경우 태그를 소지하고 있는 사용자나 태그가 부착된 물품의 위치 추적이 가능하다. 제안한 프로토콜에서는 리더와 태그사이의 모든 과정에서 태그는 랜덤 생성기와 ID_p값의 갱신을 통하여 항상 다른 값을 리더에게 보내기 때문에 위치 추적의 문제를 해결할 수 있다.

5.1.4 상호인증(Mutual Authentication)

먼저 리더가 태그를 인증하는 과정은 operation 2, 3과정을 통하여 이루어진다. 다음 태그가 리더를 인증하는 과정은 operation 3, 4과정을 통하여 이루어진다. 이로서 리더(태그)가 태그(또는 리더)를 동시에 서로를 정당한 개체라고 인증한다. 상호인증을 통하여 공격자는 리더나 태그에 대해 위조할 수 없게 된다.

5.1.5 대칭키 K의 노출에 따른 위험[14]

대칭키 기반의 인증 프로토콜에서는 대칭키를 서로 공유하고 있어야하므로 대칭키가 노출이 되면 시스템 전반 또는 하나의 태그에 문제점이 발생한다. 이 문제점을 해결하기 위해 매 세션마다 키를 변환하는 프로토콜들이 제안되었으나 동기화 문제점이 발생하였다. 제안한 프로토콜에서는 PUF를 이용하여 입력 값에 해당하는 출력 값을 대칭키로 사용하므로 키 값을 알아내기 위해서는 공격자가 태그의 PUF에 대한 모든 $CRP_1(C_1,X_1)$쌍을 유추해야 한다. 하지만 매 세션마다 다른 CRP(C1,X1) 쌍을 사용하기 때문에 이를 유추하기란 불가능하다.(하나의 태그에 사용되는 $CRP_1(C_i,X_i)$은 10^9개이다.[17]) 또한 하나의 쌍을 공격자가 알게 되어 키 값이 노출되더라도 태그가 보내는 $H(ID_i)$ 값 자체는 의미가 없다. DB의 $H(ID_i)$와 ID_i 테이블을 모른다면 ID_i값을 알 수가 없다. $H(ID_i)$를 DB에 질의하여 ID_i값을 알지 않는 한 정확한 값을 알 수가 없다. 그러므로 키가 노출이 된다 하더라도 태그 ID_i값은 노출될 위험이 없다.

<표 2>는 기존의 제안된 프로토콜인 Randomized Hash-Lock[1](①), Advanced mutual-authentication[13](②), Secure RFID mutual authentication scheme(Protocol I)(Protocol II)[26](③,④)와 본 논문에서 제안한 protocol(⑤)의 안전성을 도청, 재전송 공격, 위치 추적, 상호 인증, 키 노출 시에 따른 위험 및 동기화 문제 측면에서 분석 비교한 결과이다. 기존에 제안된 프로토콜의 안전성에 대한 분석은 앞의 관련 연구에서 이미 언급한 바 있다.

〈표 2〉 기존의 보안기법과 안전성 분석 비교

구분	① Ref [1]	② Ref [11]	③ Ref [26] Protocol I	④ Ref [26] Protocol II	⑤ Our Protocol
도청	unsafe	safe	normal	normal	safe
재전송공격	unsafe	safe	normal	normal	safe
위치추적	safe	safe	normal	normal	safe
상호인증	X	○	○	○	○
키 노출에 따른 위험	-	unsafe	unsafe	unsafe	safe
동기화 문제	-	unsafe	safe	safe	safe

* 범례 : X : 불만족, ○ : 만족

6. 효율성 분석

기존의 제안된 프로토콜과 제안한 프로토콜의 효율성을 비교하기 위하여 DB 및 리더의 연산량, 태그에서의 Hash함수 작동 횟수, 태그에서의 AES 암·복호화 작동 횟수, 태그에서의 XOR연산 횟수, 태그에서의 랜덤 넘버 생성 횟수, 인증을 위한 서버의 필요 여부를 비교 분석한 결과를 <표 3>에 나타내었다. DB 및 리더의 연산량을 비교해 보면 ① 및 ④의 제안된 프로토콜은 태그의 수만큼 검색하는데 반해 ②, ③ 및 ⑤ (제안한 프로토콜)의 DB 연산량은 O(1)이다. 따라서 ① 및 ④의 제안 프로토콜은 태그의 수가 증가하는 만큼 DB 또는 리더에 과도한 부하를 줄 수 있다. 또한 ①의 경우 태그에서의 연산량은 한번의 Hash 함수계산과 랜덤 넘버를 생성뿐 이지만 안전성 측면에서 상당히 취약함을 관련연구에서 밝힌 바 있다. ③, ④의 경우 태그에서 Hash 함수 계산을 3번, 2번을 수행하고 있으므로 수동형 태그에는 적합하지 않음을 알 수 있다. 또한 안전성 분석에서도 본 논문에서 제안한 프로토콜보다 안전하지 못함을 볼 수 있었다. 하지만 ②의 경우 본 논문에서 제안한 대칭키 기반의 프로토콜을 사용하고 있으며 안전성 측면에서도 ①, ③ 및 ④보다 안전하다. 따라서 ②의 제안된 프로토콜과 본 논문에서 제안한 프로토콜을 비교 분석한다. ② 및 ⑤를 비교하면, 태그에서 수행되는 AES 암·복호화 횟수가 각각 3E : 3E+1D

〈표 3〉 기존의 보안기법과 효율성 분석비교

구분	① Ref [1]	② Ref [11]	③ Ref [26] Protocol I	④ Ref [26] Protocol II	⑤ Our Protocol
DB 및 리더 연산량	O(N)-리더	O(1)	O(1)	O(N)	O(1)
Hash함수 작동수(Tag)	1	-	3	2	-
AES 작동수(tag)	-	3E	-	-	3E+1D
XOR연산(tag)	-	4	3	2	1
랜덤 넘버 생성 수(tag)	1	0	0	0	2
인증 시 서버 필요 여부	X	○	○	○	X

이다. [9]에서 암호화·복호화 클락 사이클이 대략 1:1.3으로 보고 있기 때문에 이를 기준으로 계산하면 3 : 4.3으로 제안한 프로토콜이 다소 많다. 이는 ②의 경우 상호인증과 키 변환을 하기 위해 서버의 자원을 사용하여 하지만 ⑤에서는 상호인증을 리더와 태그만으로 하기 때문이다. 한편 태그의 XOR연산의 횟수를 같이 비교해보면 ②의 경우는 전체 4회(암호화 및 키 갱신에 필요한 횟수)로 제안한 프로토콜의 1회로 3회의 XOR연산이 더 필요함을 알 수 있다. 하지만 제안한 프로토콜은 랜덤 넘버 생성수가 2회 더 많음을 볼 수 있다. 이는 ②의 경우 키 변환을 통하여 위치추적 문제 및 재전송 공격을 해결하였지만 제안한 프로토콜, ⑤에서는 랜덤 값으로 위치추적 및 재전송 공격을 해결하기 위함이다. 비록 제안한 프로토콜이 랜덤 넘버 생성수가 많지만 동기화 문제는 발생하지 않는 장점이 있다. 만약 ②의 경우, 키 변환을 통하여 위치추적 및 재전송 공격에 안전하게 설계했다 할지라도 동기화 문제가 발생 한다면 정당한 태그라고 할지라도 더 이상 사용하지 못하게 될 수도 있다. 이상 ② 및 제안한 프로토콜(⑤)을 비교할 때 ②에서 보다 한 번의 복호화 과정과 2번의 랜덤 생성을 태그에서 더 연산하지만 ⑤는 서버의 자원을 이용하지 않고 상호인증을 수행하고 랜덤 생성을 통하여 위치 추적 문제와 재전송 공격을 해결하였기 때문에 동기화 문제가 발생하지 않음을 확인할 수 있다.

7. 결 론

본 논문에서는 저가형 태그의 구현에 적합한 AES-128 및 해쉬 함수 SHA-1 기반의 상호인증 프로토콜을 제안하였다. 제안한 프로토콜은 태그에 구현하기 용이한 AES-128 대칭키 알고리즘을 인증프로토콜로 사용하고, 태그 ID를 일방향 해쉬 함수 SHA-1으로 암호화하여 사용함으로 물리적인 공격 시에 태그 ID노출을 차단할 수 있으며, 특히 PUF의 Challenge-Response 값을 활용하여 매 세션마다 공유 대칭키로 사용하기 때문에 키 노출 위험이 없는 안전한 프로토콜이다. 제안한 인증 프로토콜의 안전성에 대한 분석을 먼저 공격유형에 따라서 분석한 결과 도청, 재전송 공격 및 위치추적에서 안전하며, 특히 대칭키 노출에 따른 위험에서 안전함을 확인할 수 있었다. 효율성 측면에서 기존의 제안한 프로토콜과 비교 분석한 결과 우수한 효율성을 확인할 수 있었다.

참 고 문 헌

[1] Stepan A. Weis, Sanjay E. Sarma, Ronald L. Rivest, and Daniel W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," *Security in Pervasive Computing - SPC 2003*, LNCS 2802, pp.201-212, 2004.

[2] Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita, "Hash-Chain Based Forward-Secure Privacy Protection Scheme for Low-cost RFID," *Proceedings of the SCIS 2004*, pp.719-724, 2004.

[3] Keunwoo Rhee, Jin Kwak, Seungjoo Kim, and Dongho Won, "Challenge-Response Based RFID Authentication Protocol for Distributed Database Environment," International Conference on Security in Pervasive Computing Environments, pp.70-84, 2005. Springer.

[4] K. Osaka, T. Takagi, K. Yamazaki, and O. Takahashi, "An Efficient and Secure RFID Security Method with Ownership Transfer", *Computational Intelligence and Security, 2006 International Conference on*, Vol.2, No.1, 2006, pp.1090-1095.

[5] 류석, "공개키 기반의 디지털 콘텐츠 및 인스턴트 플레이어 보호방법연구," 정보처리학회논문지C Vol.13C, No.7, pp.837-842, 2006

[6] 김창훈, "타원곡선 암호 시스템의 고속 구현을 위한 VLSI 구조," 정보처리학회논문지C Vol.15C, No.2, pp.133-140, 2008.

[7] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer. "Strong authentication for RFID systems using AES algorithm," In Conference of Cryptographic Hardware and Embedded Systems, 2004. Proceedings, pp.357-370, Springer 2004.

[8] M. Feldhofer and Christian Rechberger, "A Case against Currently Used Hash Functions in RFID Protocols," OTM Workshops 2006, LNCS 4277, pp.372-381, 2006.

[9] 구본석, 유권호, 양상운, 장태주, 이상진, "RFID 태그를 위한 초소형 AES 연산기의 구현", 정보보호학회논문지, 제16권 제5호, pp.67-77, 2006.

[10] Chae Hoon Lim and Tymur Korkishko, "mCrtton - A Lightweight Block Cipher for Security of Low-Cost RFID Tags and Sensors," WISA 2005, LNCS 3786, pp.243-258, 2006.

[11] Deukjo Hong, Jaechul Sung, Seokhie Hong, Jongin Lim, Sangjin Lee, Bonseok Koo, Changhoon Lee, Donghoon Chang, Jesang Lee, Kitae Jeong, Hyun Kim, Jongsung Kim, and Seongtaek Chee, "HIGHT: A New Block Cipher Suitale for Low-Resource Device", CHES 2006, LNCS 4249, pp.

46-59, 2006.

[12] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshow, Yannick Seurin, and C. Vikkelsoe, "HEIGHT: PRESENT: An Ultra-Lightweight Block Cipher", CHES 2007, LNCS 4727, pp.450-466, 2007.

[13] B. Toiruul and KyungOh Lee, "An Advanced Mutual-Authentication Algorithn Using AES for RFID Systems", IJCSNS International Journal of Computer Science and Network Security, Vol.6, No.9B, pp.156-162, September, 2006

[14] KLAUS FINKENZELLER, 'RFID Handbook: Fundamentals and Application in Contactless Smart Cards and Identification', 2nd EdD.,John Wiley & Sons, Ltd. 2003, pp.223.

[15] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, V. Khandelwal, "Design and Implementation of PUF-Based 'Unclonable' RFID ICs for Anti-Counterfeiting and Security Applications", 2008 IEEE International Conference on RFID, 16-17 April, 2008, pp.58-64, Las Vegas, USA.

[16] L. Bolotnyy and G. Robins, "Physically Unclonable Function -Based Security and Privacy in RFID Systems", in Proc. IEEE International Conference on Pervasive Computing and Communications(PerCom 2007), pp.211-218, March, 2007.

[17] P.Tuyls and L. Batina, "RFID-Tags for Anti-Counterfeiting", Topics in Cryptology-CT-RSA 2006, Vol.3860, pp. 115-131.

[18] L. Kulseng, Z. Yu, Y. Wei and Y. Guan, "Lightweight Secure Search Protocols for Low-cost RFID Systems," 2009 29th IEEE International Conference on Distributed Computing Systems, pp.40-48.

[19] L. Kulseng, "Lightweight Mutual Authentication, Owner Transfer, and Secure Search Protocols for RFID Systems," A thesis for the degree of MASTER OF SCIENCE, Iowa State University, Ames, Iowa, 2009.

[20] 최은영, 최동희, 임종인, 이동훈, "저가형 RFID 시스템을 위한 효율적인 인증 프로토콜," 정보보호학회논문지 15권 5호, pp59-71, 2005.

[21] D. Nguyen Duc, J. Park, H. Lee and K. Kim, "Enhancing Security of EPCglobal Gen-2 RFID Tag against Traceability and Cloning," Proc. of SCIS 2006, Abstracts pp.97, Jan. 17~20, 2006, Hiroshima, Japan.

[22] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M. Estevez Tapiador, and Arturo Ribagorda, "LAMP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID tags," in *Proc. Second Workshop RFID Security*, July 2006.

[23] Ari Juels, "RFID Security and Privacy: A Research Survey," IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, Vol.24, No.2, Feb., 2006,

[24] Sandra Dominikus, Elisabeth Oswald, and Martin Feldhofer, "Symmetric Authentication for RFID Systems in Practice", Handout of the *Ecrypt Workshop on RFID and Lightweight Crypto*, Jul., 2005.

[25] Sungbae Ji, "RFID-enabled Extensible Authentication Framework and Its Applications," A thesis for the Degree of Master, ICU, 2008.

[26] S. Kang, D. Lee, and I. Lee, "A study on secure RFID mutual authentication scheme in pervasive computing environment" Computer Communications 31, 2008, pp.4248-4254.

박 용 수

e-mail : timpark75@knu.ac.kr
1979년 경북대학교 전자공학과(학사)
1981년 경북대학교 전자공학과(석사)
2002년 대구가톨릭대학교 전산통계학과(박사)
2007년~현 재 경북대학교 BK21 Post-Doc
관심분야 : 임베디드 시스템 설계, 정보 보호, ICA

신 주 석

e-mail : gome81@knu.ac.kr
2006년 경일대학교 컴퓨터공학과(학사)
2008년~현 재 경북대학교 전기전자컴퓨터공학부 석사과정
관심분야 : 임베디드 시스템 설계, RFID, 정보보호

최 명 실

e-mail : sil003@knu.ac.kr
1992년 경일대학교 컴퓨터공학과(학사)
2004년 경북대학교 컴퓨터공학과(석사)
2007년 경북대학교 컴퓨터공학과(박사)
2009년~현 재 대구가톨릭대학교 강의전담 교수
관심분야 : 웹구조, 웹마이닝, 분산처리, 임베디드 응용소프트웨어

정 경 호

e-mail : mccart@knu.ac.kr
2000년 대구대학교 컴퓨터정보공학부(학사)
2002년 경북대학교 컴퓨터공학과(석사)
2005년 경북대학교 컴퓨터공학과(박사)
2005년~현 재 경운대학교 컴퓨터공학과 교수
관심분야 : 임베디드 리눅스 시스템, 시스템 프로그래밍, 실시간 운영체제

안 광 선

e-mail : gsahn@knu.ac.kr
1972년 연세대학교 전기공학과(학사)
1975년 연세대학교 전자공학과(석사)
1980년 연세대학교 전자공학과(박사)
1977년~현 재 경북대학교 컴퓨터공학과 교수
관심분야 : 임베디드 시스템 설계